Exhibit A

4

5/26/2014   The Willy Report: proof of massive fraudulent trading activity at Mt. Gox, and how it has affected the price of Bitcoin | The Willy Report

Case 14-31229-sgj15   Doc 134-1   Filed 05/26/14   Entered 05/26/14 17:38:41   Desc
Exhibit A (Part 1)   Page 2 of 7

The Willy Report

The Willy Report: proof of massive fraudulent trading activity at Mt. Gox, and how it has affected the price of Bitcoin

Posted on May 25, 2014

Somewhere in December 2013, a number of traders including myself began noticing suspicious bot behavior on Mt. Gox. Basically, a random number between 10 and 20 bitcoin would be bought every 5-10 minutes, non-stop, for at least a month on end until the end of January. The bot was dubbed "Willy" at some point, which is the name I'll continue to use here. Since Willy was buying in such a recognizable pattern, I figured it would be easy to find in the Mt. Gox trading logs that were leaked about two months ago (there's a torrent of the data here). However, the logs only went as far as November 2013; luckily, I was able to detect the buying pattern in the last few days of November. Below is a compiled log of its trades on the last two days of November (from the file "2013-11_mtgox_japan.csv"):

```
30-11-2013 10:10 - UID: 832432 Type: buy Currency: USD BTC: 14.011528 Fiat: 16893.82
30-11-2013 10:19 - UID: 832432 Type: buy Currency: USD BTC: 16.18210837 Fiat: 19561.92
30-11-2013 10:29 - UID: 832432 Type: buy Currency: USD BTC: 18.34173105 Fiat: 22136.74
30-11-2013 10:35 - UID: 832432 Type: buy Currency: USD BTC: 18.19262893 Fiat: 21885.52
30-11-2013 10:45 - UID: 832432 Type: buy Currency: USD BTC: 11.24527636 Fiat: 13492.78
30-11-2013 10:52 - UID: 832432 Type: buy Currency: USD BTC: 14.5141487 Fiat: 17416.93
30-11-2013 10:58 - UID: 832432 Type: buy Currency: USD BTC: 15.805611 Fiat: 18978.39
30-11-2013 11:06 - UID: 832432 Type: buy Currency: USD BTC: 14.96578741 Fiat: 18108.31
30-11-2013 11:13 - UID: 832432 Type: buy Currency: USD BTC: 18.49346572 Fiat: 22412.65
30-11-2013 11:18 - UID: 832432 Type: buy Currency: USD BTC: 12.77630467 Fiat: 15500.85
30-11-2013 11:25 - UID: 832432 Type: buy Currency: USD BTC: 13.70319422 Fiat: 16621.72
30-11-2013 11:35 - UID: 832432 Type: buy Currency: USD BTC: 14.95640049 Fiat: 18120.95
30-11-2013 11:41 - UID: 832432 Type: buy Currency: USD BTC: 15.29944656 Fiat: 18544.72
30-11-2013 11:51 - UID: 832432 Type: buy Currency: USD BTC: 14.10583655 Fiat: 17073.18
30-11-2013 11:58 - UID: 832432 Type: buy Currency: USD BTC: 14.50627441 Fiat: 17560.1
30-11-2013 12:03 - UID: 832432 Type: buy Currency: USD BTC: 13.07979536 Fiat: 15865.66
30-11-2013 12:13 - UID: 832432 Type: buy Currency: USD BTC: 11.88053668 Fiat: 14411.04
30-11-2013 12:20 - UID: 832432 Type: buy Currency: USD BTC: 11.46523059 Fiat: 13913.0
30-11-2013 12:30 - UID: 832432 Type: buy Currency: USD BTC: 19.89610521 Fiat: 24187.39
```

Some notes on how I obtained this data: first, I removed all exact duplicate entries from the log. As noted in an earlier analysis, trades that involved a user ID "THK" – whose likely role was to facilitate cross-currency trades – were erroneously duplicated in the logs. Second, since the log contains an entry for each individual user-to-user trade, I aggregated every pair of trades involving the same user that occurred within 2 seconds from each other, assuming these belonged to the same market buy/sell (2 seconds to account for trading engine lag, which God knows was sometimes enormous on Mt. Gox).

You may note that these are actually multiple user IDs (denoted with "UID"); Willy was not a single account, its trading activity was spread over many accounts. Perhaps this is why others had been unable to find him in the database: there were plenty of people who knew of its existence (in fact the OP of this thread allegedly coined the name "Willy"). I noticed here that all of these accounts had one thing in common; the User_Country and User_State field both had "??" as entry. This was unusual. Normally, these fields contained country/state FIPS codes (for verified users?), nothing (unverified users?), or "!!" (users who failed verification or suspicious users?).

So I went back and gathered all of these "??" users, aggregated their trades, and summed the amount of BTC that each of these accounts bought (they never performed a single sell). They seamlessly connected to each other: when one user became inactive, the next became active usually within a few hours. Their trading

Follow

activity went back all the way to ⸻⸻⸻⸻⸻⸻ cord of trades you can see below:

Follow "The Willy Report"

Get every new post delivered to your Inbox.

Enter your email address

Sign me up

Powered by WordPress.com

```
27-9-2013 13:41 - UID: 807884 Type: buy                        iat: 5183.15
27-9-2013 13:42 - UID: 807884 Type: buy                        iat: 10615.65
27-9-2013 13:50 - UID: 807884 Type: buy                        iat: 17103.01
27-9-2013 13:58 - UID: 807884 Type: buy                        iat: 9138.56
27-9-2013 14:05 - UID: 807884 Type: buy                        at: 1988.84
27-9-2013 14:15 - UID: 807884 Type: buy                        at: 7783.81
27-9-2013 14:27 - UID: 807884 Type: buy                        Fiat: 16724.02
27-9-2013 14:35 - UID: 807884 Type: buy                        at: 12697.49
27-9-2013 14:48 - UID: 807884 Type: buy                        at: 6683.61
27-9-2013 14:56 - UID: 807884 Type: buy                        iat: 3203.12
27-9-2013 15:07 - UID: 807884 Type: buy                        iat: 5454.27
27-9-2013 15:18 - UID: 807884 Type: buy                        iat: 2933.12
27-9-2013 15:32 - UID: 807884 Type: buy                        iat: 9966.66
27-9-2013 15:43 - UID: 807884 Type: buy  Currency: USD BTC: 87.01885901 Fiat: 12003.33
27-9-2013 15:48 - UID: 807884 Type: buy  Currency: USD BTC: 144.3968184 Fiat: 19918.03
27-9-2013 16:01 - UID: 807884 Type: buy  Currency: USD BTC: 61.32151277 Fiat: 8461.08
27-9-2013 16:08 - UID: 807884 Type: buy  Currency: USD BTC: 49.70599427 Fiat: 6859.43
27-9-2013 16:22 - UID: 807884 Type: buy  Currency: USD BTC: 30.88567469 Fiat: 4262.15
```

And a compilation of when each account was active, how much BTC they bought, and how much USD they spent, with some totals at the bottom:

```
User_ID: 807884
User: a6e1c702-e6b2-4585-bdaf-d1f00e6e7db2
Start: 27-9-2013 13:41
End: 1-10-2013 0:30
BTC bought: 17650.499699839987
USD spent: 2500000.0


User_ID: 658152
User: c1ac7aeb-ac34-49cd-8363-c4bcb36a2b9f
Start: 10-10-2013 0:49
End: 15-10-2013 1:53
BTC bought: 17348.26542219
USD spent: 2500000.0


User_ID: 659582
User: b337d02a-ccd5-4323-933d-35e59d228825
```

So basically, each time, (1) an account was created, (2) the account spent some very exact amount of USD to market-buy coins ($2,500,000 was most common), (3) a new account was created very shortly after. Repeat. In total, a staggering ~$112 million was spent to buy close to 270,000 BTC – the bulk of which was bought in November. So if you were wondering how Bitcoin suddenly appreciated in value by a factor of 10 within the span of one month, well, this is why. Not Chinese investors, not the Silkroad bust – these events may have contributed, but they certainly were not the main reason. But more on that later.

At this point, I noticed that the first Willy account (created on September 27th) unlike all the others had some crazy high user ID: 807884, even though regular accounts at that point only went up to 650000 or so. So I went looking for other unusually high user IDs within that month, and lo and behold, there was another time-traveller account with an ID of 698630 – and this account, after being active for close to 8 months, became completely inactive just **7 hours** before the first Willy account became active! So it is a reasonable assumption that these accounts were controlled by the same entity. Account 698630 actually had a registered country and state: "JP", "40″ – the FIPS code for Tokyo, Japan. So I went and compiled all trades for this account. For convenience, I will dub this user "Markus". Its trades are as follows:

```
14-2-2013 3:37 - UID: 698630 Type: buy Currency: USD BTC: 2500.00000006 Fiat: 6600.01
14-2-2013 3:37 - UID: 698630 Type: buy Currency: USD BTC: 2500.00000003 Fiat: 258373.84
14-2-2013 3:39 - UID: 698630 Type: buy Currency: USD BTC: 500.0 Fiat: 187.76
14-2-2013 3:42 - UID: 698630 Type: buy Currency: USD BTC: 500.00000003 Fiat: 16.06
14-2-2013 3:53 - UID: 698630 Type: buy Currency: USD BTC: 500.0 Fiat: 2279.47
14-2-2013 3:54 - UID: 698630 Type: buy Currency: USD BTC: 499.99999999 Fiat: 400.44
14-2-2013 3:56 - UID: 698630 Type: buy Currency: USD BTC: 499.99999999 Fiat: 2.04
14-2-2013 3:57 - UID: 698630 Type: buy Currency: USD BTC: 500.00000001 Fiat: 192.08
14-2-2013 3:58 - UID: 698630 Type: buy Currency: USD BTC: 2500.00000004 Fiat: 1012.72
14-2-2013 4:15 - UID: 698630 Type: buy Currency: USD BTC: 499.99999997 Fiat: 1565.39
14-2-2013 4:16 - UID: 698630 Type: buy Currency: USD BTC: 1000.0 Fiat: 19961.94
14-2-2013 4:18 - UID: 698630 Type: buy Currency: USD BTC: 1000.0 Fiat: 104.08
14-2-2013 4:23 - UID: 698630 Type: buy Currency: USD BTC: 2000.00000035 Fiat: 2133.29
14-2-2013 4:25 - UID: 698630 Type: buy Currency: USD BTC: 2499.99999998 Fiat: 35675.81
14-2-2013 4:37 - UID: 698630 Type: buy Currency: USD BTC: 1000.00000005 Fiat: 29962.32
14-2-2013 4:40 - UID: 698630 Type: buy Currency: USD BTC: 768.51248974 Fiat: 504.59
19-2-2013 1:00 - UID: 698630 Type: buy Currency: USD BTC: 331.36211505 Fiat: 11577.17
19-2-2013 1:00 - UID: 698630 Type: buy Currency: USD BTC: 2168.63788501 Fiat: 21526.3
```

There were several peculiar things about Markus. First, its fees paid were always 0. Second, its fiat spent when buying coins was all over the place, with seemingly completely random prices paid per bitcoin. For reference, Markus is the "Glitch in the System" user in this excellent Gox DB visualization (on that note, all of the Willy accounts are the "Greater Fools" with just big green blotches around Oct-Nov). Upon further inspection of the log, it became clear what was the cause of these seemingly random values:

In this table, the first two trades (buy/sell pairs) are by some regular user with ID 238168. In the second trade, this user buys 0.398 BTC for $15.13. The next trade is some large market buy by Markus (ID 698630): note how the "$15.13" value from the previous trade seems to "stick"; regardless of the volume of BTC bought, the value paid is always $15.13. This is speculation, but perhaps for Markus, the "Money" spent field is in fact empty, and the program that generates the trading logs simply takes whatever value was already there before. In other words, Markus is somehow buying tons of BTC without spending a dime. Interestingly, Markus also sells every now and then, and for some reason the price values are correct this case. His biggest sell occurred on June 2nd. I've analyzed these trades separately here:

```
2-6-2013 8:22 - UID: 698630 Type: sell Currency: USD BTC: 1998.98799992 Fiat: 254788.4
2-6-2013 8:23 - UID: 698630 Type: sell Currency: USD BTC: 999.99999997 Fiat: 127026.48
2-6-2013 8:23 - UID: 698630 Type: sell Currency: USD BTC: 1000.0 Fiat: 127002.4
2-6-2013 8:24 - UID: 698630 Type: sell Currency: USD BTC: 1000.0 Fiat: 127018.51
2-6-2013 8:24 - UID: 698630 Type: sell Currency: USD BTC: 1000.0 Fiat: 127001.35
2-6-2013 8:24 - UID: 698630 Type: sell Currency: USD BTC: 1000.00000005 Fiat: 127004.44
2-6-2013 8:24 - UID: 698630 Type: sell Currency: USD BTC: 1000.0 Fiat: 127000.0
2-6-2013 8:24 - UID: 698630 Type: sell Currency: USD BTC: 1000.00000003 Fiat: 127001.4
2-6-2013 8:24 - UID: 698630 Type: sell Currency: USD BTC: 1000.0 Fiat: 127000.0
2-6-2013 8:24 - UID: 698630 Type: sell Currency: USD BTC: 999.99999998 Fiat: 126894.45
2-6-2013 8:24 - UID: 698630 Type: sell Currency: USD BTC: 1000.0 Fiat: 126500.0
2-6-2013 8:25 - UID: 698630 Type: sell Currency: USD BTC: 999.99999998 Fiat: 126417.04
2-6-2013 8:26 - UID: 698630 Type: sell Currency: USD BTC: 995.0 Fiat: 125339.88
2-6-2013 8:26 - UID: 698630 Type: sell Currency: USD BTC: 1847.3314792 Fiat: 231285.05
2-6-2013 8:28 - UID: 698630 Type: sell Currency: USD BTC: 694.77000953 Fiat: 86753.84
2-6-2013 8:30 - UID: 698630 Type: sell Currency: USD BTC: 1766.9595302 Fiat: 215912.72
2-6-2013 8:32 - UID: 698630 Type: sell Currency: USD BTC: 2344.29615506 Fiat: 283975.16
2-6-2013 8:36 - UID: 698630 Type: sell Currency: USD BTC: 191.90340171 Fiat: 23243.51
```

Sell 31k BTC, receive $4 million, re-buy 15k BTC, spend nothing. Awesome! Here is the corresponding chart for this day, just to show that these trades (from 8:00 to 10:00 am) actually occurred "on-market", and had a significant effect on the price.

Some totals compiled for Markus:

```
Start: 14-2-2013 3:37
End: 27-9-2013 6:16
User_ID: 698630
User: b2853e3c-3ec0-4fa5-8231-d21e2fd13330

BTC bought: 335203.83080579044
USD spent: $??.??
JPY spent: 0.0
EUR spent: €2110.46

BTC sold: 37575.39028677996
USD received: $4,018,376.87
JPY received: ¥2,744,463.91
EUR received: 0.0
```

Another net ~300,000 BTC bought. Combined with Willy's buys, that's around 570,000 BTC in total. Although there are no trading logs after November, Willy was observed by multiple traders to be active for the most part of December until the end of January as well. Although this was at a slower, more consistent pace (around 2000 BTC per day), it should roughly add up to another 80,000 BTC or so bought. So that's a total that's suspiciously close to the supposedly lost ~650,000 BTC.

So... hacker, or inside job?

At this point, I guess the straightforward conclusion would be that this is how the coins were stolen: a hacker gained access to the system or database, was able to assign himself accounts with any amount of USD at will, and just started buying and withdrawing away. This is in line with what GoxDox.org reported last month (they leaked the Sunlot court filing, so clearly they have some inside info). After all, the constant creation of new Willy accounts seems almost intended to avoid detection. Unverified BTC withdrawals may have been possible until late 2013 (I could not find any exact data on this), or perhaps the "??" location values in the database (unlike the usual empty or "!!" values for unverified users) were able to fool the system into thinking this user was verified. However, there are a lot of things that don't add up with this theory; in fact there is a ton of evidence to suggest that all of these accounts were controlled by Mt. Gox themselves.

First, the obvious: Markus has Tokyo, Japan as its registered location. But any hacker could edit a DB entry to

5/26/2014 The Willy Report: proof of massive fraudulent trading activity at Mt. Gox, and how it has affected the price of Bitcoin | The Willy Report

Case 14-31229-sgj15 Doc 134-1 Filed 05/26/14 Entered 05/26/14 17:38:41 Desc
Exhibit A (Part 1) Page 6 of 7

try and frame someone (or even be located in Tokyo, however unlikely). However, none of the Willy accounts until November appear in the leaked balance summary at the time of collapse, and there seem to be no corresponding withdrawals for those amounts of bitcoin bought. Markus does have a balance: around 20 BTC and small amounts of EUR, JPY and **PLN**. No USD balance. In other words, only currencies for which Mt. Gox actively controlled bank accounts.

The next piece of evidence is perhaps more convincing. For some months in 2013, there were two versions of trading logs in the leaked database: a full log, and an anonymized log with user hashes and country/state codes removed. For April 2013, there was a .zip file which contained one such anonymized log – this is speculation, but one use of this may have been to send off to auditors/investors to show some internals. Upon closer inspection, it turns out the full and anonymized versions of all the logs differ in two, and ONLY two ways:

1. User hashes and country/state codes are removed.
2. **Markus' out-of-place user ID (698630) is changed to a small number (634), and its strange fixed "Money" values are corrected to the expected values**.

Interesting detail: from the 2011 leaked account list, the user with ID 634 has username "MagicalTux". Compare these two tables:

The "fixed" file has an earlier creation date than the full log, so it could not have been a reporting bug that was fixed later. Everything points to these values having been manually edited, presumably to erase traces of suspicious activity. Although another possibility is that it is actually the other way around – the correct log with earlier creation date was the original, and all other logs have been altered to a different ID not traceable to MagicalTux to cover up fraud in a very lazy way (by setting all Money spent to whatever was the last trade), and someone forgot there was still a zip file lying around with the unaltered data.

Another thing: Willy seemed to be immune to network downtime.
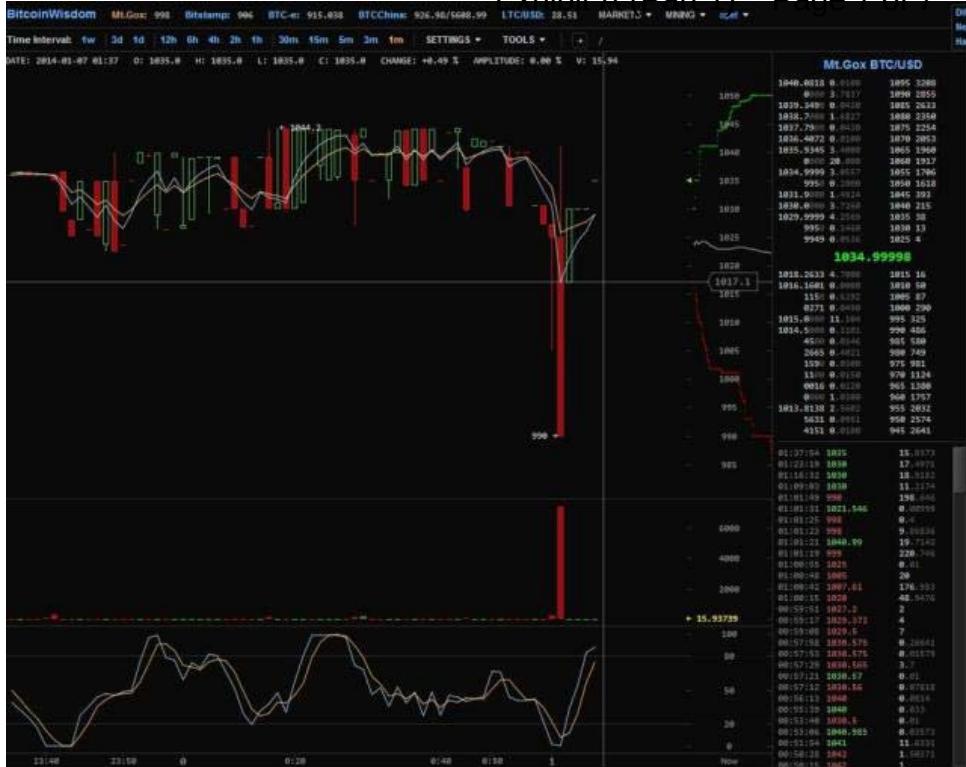
The latest four trades displayed in the bottom-right corner showcase Willy's typical trading activity observed from December onwards: a 10-20 BTC buy every 5-10 minutes. At a time no one else was able to trade, be it via API or otherwise, Willy was somehow able to continue as if nothing ever happened. This makes it likely the bot was being run from a local Mt. Gox server. It is not impossible that a hacker was able to install some kind of rootkit on Mt. Gox's servers and ran the bot from there, but that seems extremely unlikely.

Before Markus

Of course, I was curious to see if the April 2013 bubble was just as fake as the November 2013 bubble was (as should be evident from the above data, and the more detailed price analysis below). Although I could find no clear single buy bot active during the February-April run up (Markus bought a significant amount of coins, but not enough to sustain the prolonged rally), there was still tons of suspicious activity in the log. When browsing through the trading data sorted by user ID, I noticed a huge number of active "Japan" users with very low user IDs (<1000). None were paying fees. Odd to say the least, so I investigated further. Turns out a lot of these trades followed a very distinct pattern, and were unlikely to have been executed by their original account holders, but rather these accounts were "hijacked" in some way. The image below shows an example of this pattern:

First, a user with ID 179200 (highlighted; it is always this user as far as I can tell) buys some very exact amount of JPY worth of BTC (in this case JPY 24000) from regular users.

Immediately after, a mysterious low-ID JP user also buys up some exact amount of JPY worth of BTC (always several times more than what user 179200 bought). This happens over and over again, for different low-ID users. But here's the interesting thing: the user _hashes_ for these low ID JP users do not add up with the user hashes of the original account holders. Look at this:

The data is sorted by user ID. Highlighted is the likely original, legit user making a legit trade. The hash is